9 JAN 1978

COMMENTS AND THOUGHTS FROM READING THE BOOK,

THE MAN WHO BROKE PURPLE, BY RONALD CLARK

STAT

1. William Freedman believed there was no cipher system that could not be broken down nor did he believe that big computers were of much use in cryptoanalysis. It appears he was out of date on this latter point, but particularly when you take into account that computers can be used for cryptoanalysis it may strengthen his first point.

a. How do we use computers for cryptoanalysis?

b. How can we be confident that our systems are not compromised?

(1) What protections do we have for super secret information? Is the encryption different?

(2) What do we do to check whether our systems are breakable or not? Do we actually attempt to exploit them with some of the same diligence we do other systems?

(3) What do we know about the size and extent of the Soviets' cryptoanalysis endeavor -- its history and its present configuration?

STAT

2. (Page 114). It was 1929 when Henry Stimson said that "gentlemen do not read each others mail." Immediately thereafter, at State Department initiative, the "Black Chamber" cryptoanalytic organization was disestablished. In May 1929, the Christian Science Monitor commented: "This fine gesture will commend itself to all who are trying to develop the same standards of decency between governments as exists between individuals."

a. Fortunately the work of the Black Chamber went on in other guises. What do we know about our

[redacted]

STAT

3. When we entered World War II we certainly did not have any cryptographic systems which Freedman thought were truly secure. We simply used the best we could. The book does not make it clear whether Freedman feels we ever did develop totally secure systems. How can we be quite so confident today?

4. When there was a leak through the Chicago Tribune on our having broken Purple, there were two side effects:

a. Distribution of Purple material was drastically cut down and this may have affected the analysis for the Pearl Harbor situation.

b. It opened up the possibility of the Japanese sending deliberately misleading messages which they knew we were deciphering.

When Mrs. Freedman became the principal cryptographer in 1941 for OSS, she instituted the secrecy oath.